INTERNATIONAL STANDARD

**ISO 31000**

Second edition
2018-02

# Risk management — Guidelines

*Management du risque — Lignes directrices*

Reference number
ISO 31000:2018(E)

© ISO 2018

Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

## COPYRIGHT PROTECTED DOCUMENT

© ISO 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

# Contents

Page

**Foreword** ... **iv**
**Introduction** ... **v**
**1 Scope** ... **1**
**2 Normative references** ... **1**
**3 Terms and definitions** ... **1**
**4 Principles** ... **2**
**5 Framework** ... **4**
5.1 General ... 4
5.2 Leadership and commitment ... 5
5.3 Integration ... 5
5.4 Design ... 6
5.4.1 Understanding the organization and its context ... 6
5.4.2 Articulating risk management commitment ... 6
5.4.3 Assigning organizational roles, authorities, responsibilities and accountabilities 7
5.4.4 Allocating resources ... 7
5.4.5 Establishing communication and consultation ... 7
5.5 Implementation ... 7
5.6 Evaluation ... 8
5.7 Improvement ... 8
5.7.1 Adapting ... 8
5.7.2 Continually improving ... 8
**6 Process** ... **8**
6.1 General ... 8
6.2 Communication and consultation ... 9
6.3 Scope, context and criteria ... 10
6.3.1 General ... 10
6.3.2 Defining the scope ... 10
6.3.3 External and internal context ... 10
6.3.4 Defining risk criteria ... 10
6.4 Risk assessment ... 11
6.4.1 General ... 11
6.4.2 Risk identification ... 11
6.4.3 Risk analysis ... 12
6.4.4 Risk evaluation ... 12
6.5 Risk treatment ... 13
6.5.1 General ... 13
6.5.2 Selection of risk treatment options ... 13
6.5.3 Preparing and implementing risk treatment plans ... 14
6.6 Monitoring and review ... 14
6.7 Recording and reporting ... 14
**Bibliography** ... **16**

© ISO 2018 – All rights reserved


Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

# Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 262, *Risk management*.

This second edition cancels and replaces the first edition (ISO 31000:2009) which has been technically revised.

The main changes compared to the previous edition are as follows:

— review of the principles of risk management, which are the key criteria for its success;

— highlighting of the leadership by top management and the integration of risk management, starting with the governance of the organization;

— greater emphasis on the iterative nature of risk management, noting that new experiences, knowledge and analysis can lead to a revision of process elements, actions and controls at each stage of the process;

— streamlining of the content with greater focus on sustaining an open systems model to fit multiple needs and contexts.


© ISO 2018 – All rights reserved

Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

# Introduction

This document is for use by people who create and protect value in organizations by managing risks, making decisions, setting and achieving objectives and improving performance.

Organizations of all types and sizes face external and internal factors and influences that make it uncertain whether they will achieve their objectives.

Managing risk is iterative and assists organizations in setting strategy, achieving objectives and making informed decisions.

Managing risk is part of governance and leadership, and is fundamental to how the organization is managed at all levels. It contributes to the improvement of management systems.

Managing risk is part of all activities associated with an organization and includes interaction with stakeholders.

Managing risk considers the external and internal context of the organization, including human behaviour and cultural factors.

Managing risk is based on the principles, framework and process outlined in this document, as illustrated in Figure 1. These components might already exist in full or in part within the organization, however, they might need to be adapted or improved so that managing risk is efficient, effective and consistent.

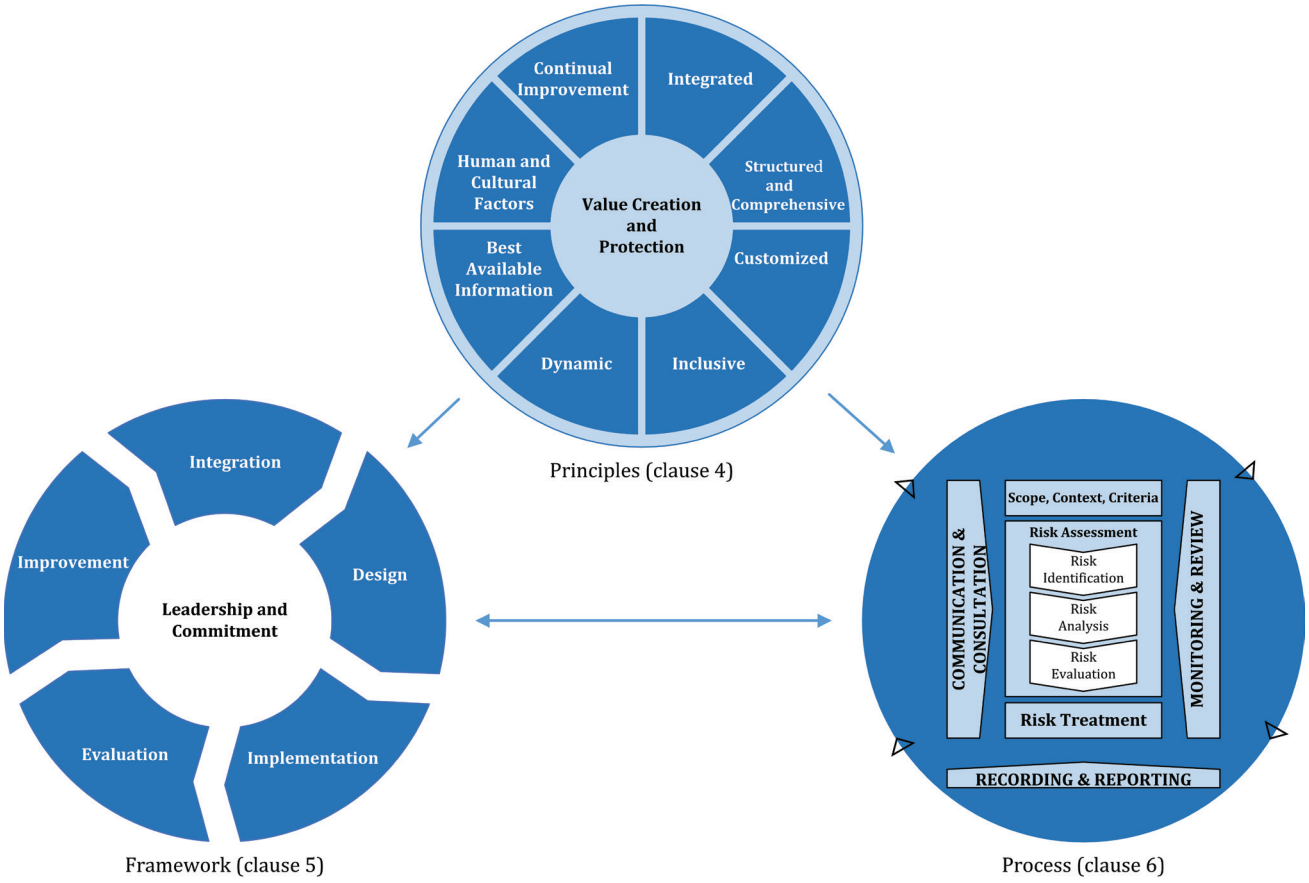


**Figure 1 — Principles, framework and process**

© ISO 2018 – All rights reserved


Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by  University of Toronto User.  No further reproduction or distribution is permitted.

# Risk management — Guidelines

## 1 Scope

This document provides guidelines on managing risk faced by organizations. The application of these guidelines can be customized to any organization and its context.

This document provides a common approach to managing any type of risk and is not industry or sector specific.

This document can be used throughout the life of the organization and can be applied to any activity, including decision-making at all levels.

## 2 Normative references

There are no normative references in this document.

## 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org

**3.1**
**risk**
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of *risk sources* (3.4), potential *events* (3.5), their *consequences* (3.6) and their *likelihood* (3.7).

**3.2**
**risk management**
coordinated activities to direct and control an organization with regard to *risk* (3.1)

**3.3**
**stakeholder**
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Note 1 to entry: The term “interested party” can be used as an alternative to “stakeholder”.

**3.4**
**risk source**
element which alone or in combination has the potential to give rise to *risk* (3.1)

© ISO 2018 – All rights reserved


Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

**3.5**
**event**
occurrence or change of a particular set of circumstances

Note 1 to entry: An event can have one or more occurrences, and can have several causes and several *consequences* (3.6).

Note 2 to entry: An event can also be something that is expected which does not happen, or something that is not expected which does happen.

Note 3 to entry: An event can be a risk source.

**3.6**
**consequence**
outcome of an *event* (3.5) affecting objectives

Note 1 to entry: A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.

Note 2 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 3 to entry: Any consequence can escalate through cascading and cumulative effects.

**3.7**
**likelihood**
chance of something happening

Note 1 to entry: In *risk management* (3.2) terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Note 2 to entry: The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

**3.8**
**control**
measure that maintains and/or modifies *risk* (3.1)

Note 1 to entry: Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

## 4 Principles

The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives.

The principles outlined in Figure 2 provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose. The principles are the foundation for managing risk and should be considered when establishing the organization's risk management framework and processes. These principles should enable an organization to manage the effects of uncertainty on its objectives.


© ISO 2018 – All rights reserved

Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

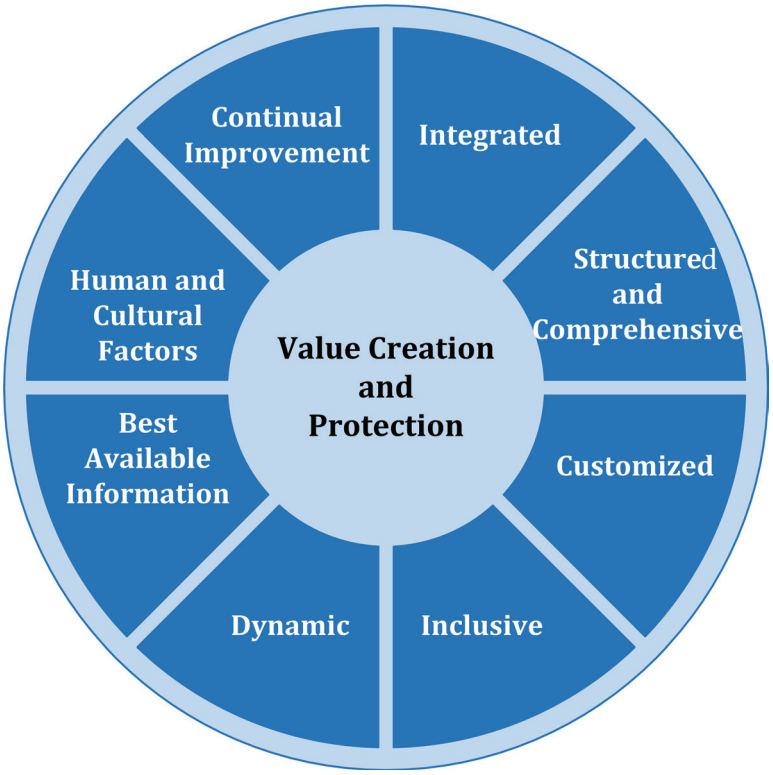


**Figure 2 — Principles**

Effective risk management requires the elements of Figure 2 and can be further explained as follows.

a) Integrated

Risk management is an integral part of all organizational activities.

b) Structured and comprehensive

A structured and comprehensive approach to risk management contributes to consistent and comparable results.

c) Customized

The risk management framework and process are customized and proportionate to the organization's external and internal context related to its objectives.

d) Inclusive

Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.

e) Dynamic

Risks can emerge, change or disappear as an organization's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.

f) Best available information

The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.

© ISO 2018 – All rights reserved


Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

g) Human and cultural factors

Human behaviour and culture significantly influence all aspects of risk management at each level and stage.

h) Continual improvement

Risk management is continually improved through learning and experience.

# 5 Framework

## 5.1 General

The purpose of the risk management framework is to assist the organization in integrating risk management into significant activities and functions. The effectiveness of risk management will depend on its integration into the governance of the organization, including decision-making. This requires support from stakeholders, particularly top management.

Framework development encompasses integrating, designing, implementing, evaluating and improving risk management across the organization. Figure 3 illustrates the components of a framework.

**Figure 3 — Framework**

The organization should evaluate its existing risk management practices and processes, evaluate any gaps and address those gaps within the framework.

The components of the framework and the way in which they work together should be customized to the needs of the organization.


© ISO 2018 – All rights reserved

Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

## 5.2 Leadership and commitment

Top management and oversight bodies, where applicable, should ensure that risk management is integrated into all organizational activities and should demonstrate leadership and commitment by:

— customizing and implementing all components of the framework;

— issuing a statement or policy that establishes a risk management approach, plan or course of action;

— ensuring that the necessary resources are allocated to managing risk;

— assigning authority, responsibility and accountability at appropriate levels within the organization.

This will help the organization to:

— align risk management with its objectives, strategy and culture;

— recognize and address all obligations, as well as its voluntary commitments;

— establish the amount and type of risk that may or may not be taken to guide the development of risk criteria, ensuring that they are communicated to the organization and its stakeholders;

— communicate the value of risk management to the organization and its stakeholders;

— promote systematic monitoring of risks;

— ensure that the risk management framework remains appropriate to the context of the organization.

Top management is accountable for managing risk while oversight bodies are accountable for overseeing risk management. Oversight bodies are often expected or required to:

— ensure that risks are adequately considered when setting the organization's objectives;

— understand the risks facing the organization in pursuit of its objectives;

— ensure that systems to manage such risks are implemented and operating effectively;

— ensure that such risks are appropriate in the context of the organization's objectives;

— ensure that information about such risks and their management is properly communicated.

## 5.3 Integration

Integrating risk management relies on an understanding of organizational structures and context. Structures differ depending on the organization's purpose, goals and complexity. Risk is managed in every part of the organization's structure. Everyone in an organization has responsibility for managing risk.

Governance guides the course of the organization, its external and internal relationships, and the rules, processes and practices needed to achieve its purpose. Management structures translate governance direction into the strategy and associated objectives required to achieve desired levels of sustainable performance and long-term viability. Determining risk management accountability and oversight roles within an organization are integral parts of the organization's governance.

Integrating risk management into an organization is a dynamic and iterative process, and should be customized to the organization's needs and culture. Risk management should be a part of, and not separate from, the organizational purpose, governance, leadership and commitment, strategy, objectives and operations.

© ISO 2018 – All rights reserved


Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

## 5.4 Design

### 5.4.1 Understanding the organization and its context

When designing the framework for managing risk, the organization should examine and understand its external and internal context.

Examining the organization's external context may include, but is not limited to:

— the social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, whether international, national, regional or local;

— key drivers and trends affecting the objectives of the organization;

— external stakeholders' relationships, perceptions, values, needs and expectations;

— contractual relationships and commitments;

— the complexity of networks and dependencies.

Examining the organization's internal context may include, but is not limited to:

— vision, mission and values;

— governance, organizational structure, roles and accountabilities;

— strategy, objectives and policies;

— the organization's culture;

— standards, guidelines and models adopted by the organization;

— capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, intellectual property, processes, systems and technologies);

— data, information systems and information flows;

— relationships with internal stakeholders, taking into account their perceptions and values;

— contractual relationships and commitments;

— interdependencies and interconnections.

### 5.4.2 Articulating risk management commitment

Top management and oversight bodies, where applicable, should demonstrate and articulate their continual commitment to risk management through a policy, a statement or other forms that clearly convey an organization's objectives and commitment to risk management. The commitment should include, but is not limited to:

— the organization's purpose for managing risk and links to its objectives and other policies;

— reinforcing the need to integrate risk management into the overall culture of the organization;

— leading the integration of risk management into core business activities and decision-making;

— authorities, responsibilities and accountabilities;

— making the necessary resources available;

— the way in which conflicting objectives are dealt with;

— measurement and reporting within the organization's performance indicators;


© ISO 2018 – All rights reserved

Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

— review and improvement.

The risk management commitment should be communicated within an organization and to stakeholders, as appropriate.

### 5.4.3 Assigning organizational roles, authorities, responsibilities and accountabilities

Top management and oversight bodies, where applicable, should ensure that the authorities, responsibilities and accountabilities for relevant roles with respect to risk management are assigned and communicated at all levels of the organization, and should:

— emphasize that risk management is a core responsibility;

— identify individuals who have the accountability and authority to manage risk (risk owners).

### 5.4.4 Allocating resources

Top management and oversight bodies, where applicable, should ensure allocation of appropriate resources for risk management, which can include, but are not limited to:

— people, skills, experience and competence;

— the organization's processes, methods and tools to be used for managing risk;

— documented processes and procedures;

— information and knowledge management systems;

— professional development and training needs.

The organization should consider the capabilities of, and constraints on, existing resources.

### 5.4.5 Establishing communication and consultation

The organization should establish an approved approach to communication and consultation in order to support the framework and facilitate the effective application of risk management. Communication involves sharing information with targeted audiences. Consultation also involves participants providing feedback with the expectation that it will contribute to and shape decisions or other activities. Communication and consultation methods and content should reflect the expectations of stakeholders, where relevant.

Communication and consultation should be timely and ensure that relevant information is collected, collated, synthesised and shared, as appropriate, and that feedback is provided and improvements are made.

## 5.5 Implementation

The organization should implement the risk management framework by:

— developing an appropriate plan including time and resources;

— identifying where, when and how different types of decisions are made across the organization, and by whom;

— modifying the applicable decision-making processes where necessary;

— ensuring that the organization's arrangements for managing risk are clearly understood and practised.

© ISO 2018 – All rights reserved


Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

Successful implementation of the framework requires the engagement and awareness of stakeholders. This enables organizations to explicitly address uncertainty in decision-making, while also ensuring that any new or subsequent uncertainty can be taken into account as it arises.

Properly designed and implemented, the risk management framework will ensure that the risk management process is a part of all activities throughout the organization, including decision-making, and that changes in external and internal contexts will be adequately captured.

## 5.6 Evaluation

In order to evaluate the effectiveness of the risk management framework, the organization should:

— periodically measure risk management framework performance against its purpose, implementation plans, indicators and expected behaviour;

— determine whether it remains suitable to support achieving the objectives of the organization.

## 5.7 Improvement

### 5.7.1 Adapting

The organization should continually monitor and adapt the risk management framework to address external and internal changes. In doing so, the organization can improve its value.

### 5.7.2 Continually improving

The organization should continually improve the suitability, adequacy and effectiveness of the risk management framework and the way the risk management process is integrated.

As relevant gaps or improvement opportunities are identified, the organization should develop plans and tasks and assign them to those accountable for implementation. Once implemented, these improvements should contribute to the enhancement of risk management.

# 6 Process

## 6.1 General

The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk. This process is illustrated in Figure 4.


© ISO 2018 – All rights reserved

Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

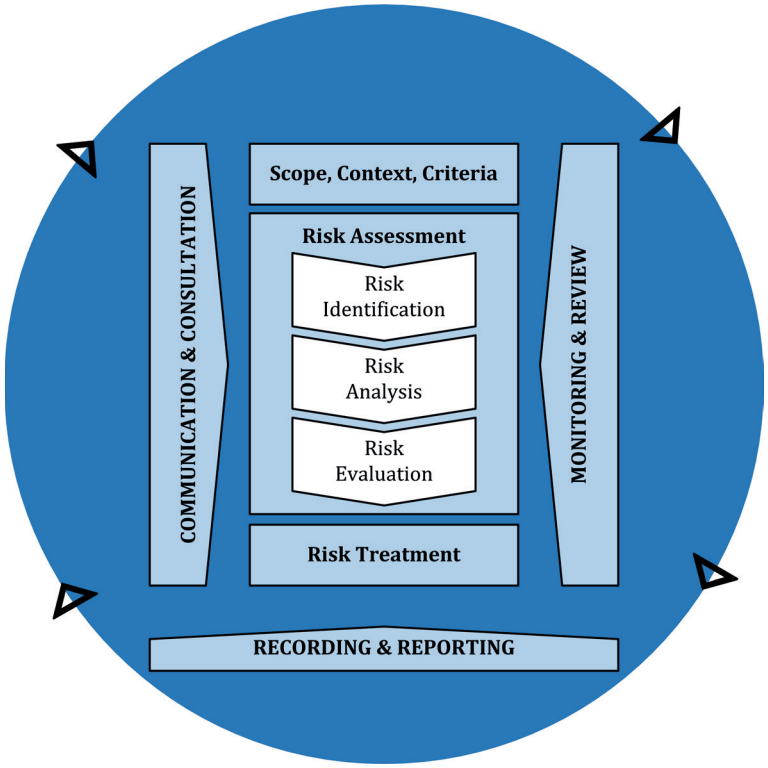


**Figure 4 — Process**

The risk management process should be an integral part of management and decision-making and integrated into the structure, operations and processes of the organization. It can be applied at strategic, operational, programme or project levels.

There can be many applications of the risk management process within an organization, customized to achieve objectives and to suit the external and internal context in which they are applied.

The dynamic and variable nature of human behaviour and culture should be considered throughout the risk management process.

Although the risk management process is often presented as sequential, in practice it is iterative.

## 6.2 Communication and consultation

The purpose of communication and consultation is to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required. Communication seeks to promote awareness and understanding of risk, whereas consultation involves obtaining feedback and information to support decision-making. Close coordination between the two should facilitate factual, timely, relevant, accurate and understandable exchange of information, taking into account the confidentiality and integrity of information as well as the privacy rights of individuals.

Communication and consultation with appropriate external and internal stakeholders should take place within and throughout all steps of the risk management process.

Communication and consultation aims to:

— bring different areas of expertise together for each step of the risk management process;

— ensure that different views are appropriately considered when defining risk criteria and when evaluating risks;

— provide sufficient information to facilitate risk oversight and decision-making;

© ISO 2018 – All rights reserved


Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

— build a sense of inclusiveness and ownership among those affected by risk.

## 6.3 Scope, context and criteria

### 6.3.1 General

The purpose of establishing the scope, the context and criteria is to customize the risk management process, enabling effective risk assessment and appropriate risk treatment. Scope, context and criteria involve defining the scope of the process, and understanding the external and internal context.

### 6.3.2 Defining the scope

The organization should define the scope of its risk management activities.

As the risk management process may be applied at different levels (e.g. strategic, operational, programme, project, or other activities), it is important to be clear about the scope under consideration, the relevant objectives to be considered and their alignment with organizational objectives.

When planning the approach, considerations include:

— objectives and decisions that need to be made;

— outcomes expected from the steps to be taken in the process;

— time, location, specific inclusions and exclusions;

— appropriate risk assessment tools and techniques;

— resources required, responsibilities and records to be kept;

— relationships with other projects, processes and activities.

### 6.3.3 External and internal context

The external and internal context is the environment in which the organization seeks to define and achieve its objectives.

The context of the risk management process should be established from the understanding of the external and internal environment in which the organization operates and should reflect the specific environment of the activity to which the risk management process is to be applied.

Understanding the context is important because:

— risk management takes place in the context of the objectives and activities of the organization;

— organizational factors can be a source of risk;

— the purpose and scope of the risk management process may be interrelated with the objectives of the organization as a whole.

The organization should establish the external and internal context of the risk management process by considering the factors mentioned in 5.4.1.

### 6.3.4 Defining risk criteria

The organization should specify the amount and type of risk that it may or may not take, relative to objectives. It should also define criteria to evaluate the significance of risk and to support decision-making processes. Risk criteria should be aligned with the risk management framework and customized to the specific purpose and scope of the activity under consideration. Risk criteria should reflect the organization's values, objectives and resources and be consistent with policies and statements


© ISO 2018 – All rights reserved

Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

about risk management. The criteria should be defined taking into consideration the organization's obligations and the views of stakeholders.

While risk criteria should be established at the beginning of the risk assessment process, they are dynamic and should be continually reviewed and amended, if necessary.

To set risk criteria, the following should be considered:

— the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible);

— how consequences (both positive and negative) and likelihood will be defined and measured;

— time-related factors;

— consistency in the use of measurements;

— how the level of risk is to be determined;

— how combinations and sequences of multiple risks will be taken into account;

— the organization's capacity.

## 6.4 Risk assessment

### 6.4.1 General

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

Risk assessment should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiry as necessary.

### 6.4.2 Risk identification

The purpose of risk identification is to find, recognize and describe risks that might help or prevent an organization achieving its objectives. Relevant, appropriate and up-to-date information is important in identifying risks.

The organization can use a range of techniques for identifying uncertainties that may affect one or more objectives. The following factors, and the relationship between these factors, should be considered:

— tangible and intangible sources of risk;

— causes and events;

— threats and opportunities;

— vulnerabilities and capabilities;

— changes in the external and internal context;

— indicators of emerging risks;

— the nature and value of assets and resources;

— consequences and their impact on objectives;

— limitations of knowledge and reliability of information;

— time-related factors;

— biases, assumptions and beliefs of those involved.

© ISO 2018 – All rights reserved


Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

The organization should identify risks, whether or not their sources are under its control. Consideration should be given that there may be more than one type of outcome, which may result in a variety of tangible or intangible consequences.

### 6.4.3 Risk analysis

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect multiple objectives.

Risk analysis can be undertaken with varying degrees of detail and complexity, depending on the purpose of the analysis, the availability and reliability of information, and the resources available. Analysis techniques can be qualitative, quantitative or a combination of these, depending on the circumstances and intended use.

Risk analysis should consider factors such as:

— the likelihood of events and consequences;

— the nature and magnitude of consequences;

— complexity and connectivity;

— time-related factors and volatility;

— the effectiveness of existing controls;

— sensitivity and confidence levels.

The risk analysis may be influenced by any divergence of opinions, biases, perceptions of risk and judgements. Additional influences are the quality of the information used, the assumptions and exclusions made, any limitations of the techniques and how they are executed. These influences should be considered, documented and communicated to decision makers.

Highly uncertain events can be difficult to quantify. This can be an issue when analysing events with severe consequences. In such cases, using a combination of techniques generally provides greater insight.

Risk analysis provides an input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods. The results provide insight for decisions, where choices are being made, and the options involve different types and levels of risk.

### 6.4.4 Risk evaluation

The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. This can lead to a decision to:

— do nothing further;

— consider risk treatment options;

— undertake further analysis to better understand the risk;

— maintain existing controls;

— reconsider objectives.

Decisions should take account of the wider context and the actual and perceived consequences to external and internal stakeholders.


© ISO 2018 – All rights reserved

Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

The outcome of risk evaluation should be recorded, communicated and then validated at appropriate levels of the organization.

## 6.5 Risk treatment

### 6.5.1 General

The purpose of risk treatment is to select and implement options for addressing risk.

Risk treatment involves an iterative process of:

— formulating and selecting risk treatment options;

— planning and implementing risk treatment;

— assessing the effectiveness of that treatment;

— deciding whether the remaining risk is acceptable;

— if not acceptable, taking further treatment.

### 6.5.2 Selection of risk treatment options

Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived in relation to the achievement of the objectives against costs, effort or disadvantages of implementation.

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Options for treating risk may involve one or more of the following:

— avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

— taking or increasing the risk in order to pursue an opportunity;

— removing the risk source;

— changing the likelihood;

— changing the consequences;

— sharing the risk (e.g. through contracts, buying insurance);

— retaining the risk by informed decision.

Justification for risk treatment is broader than solely economic considerations and should take into account all of the organization's obligations, voluntary commitments and stakeholder views. The selection of risk treatment options should be made in accordance with the organization's objectives, risk criteria and available resources.

When selecting risk treatment options, the organization should consider the values, perceptions and potential involvement of stakeholders and the most appropriate ways to communicate and consult with them. Though equally effective, some risk treatments can be more acceptable to some stakeholders than to others.

Risk treatments, even if carefully designed and implemented might not produce the expected outcomes and could produce unintended consequences. Monitoring and review need to be an integral part of the risk treatment implementation to give assurance that the different forms of treatment become and remain effective.

Risk treatment can also introduce new risks that need to be managed.

© ISO 2018 – All rights reserved


Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

If there are no treatment options available or if treatment options do not sufficiently modify the risk, the risk should be recorded and kept under ongoing review.

Decision makers and other stakeholders should be aware of the nature and extent of the remaining risk after risk treatment. The remaining risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

### 6.5.3 Preparing and implementing risk treatment plans

The purpose of risk treatment plans is to specify how the chosen treatment options will be implemented, so that arrangements are understood by those involved, and progress against the plan can be monitored. The treatment plan should clearly identify the order in which risk treatment should be implemented.

Treatment plans should be integrated into the management plans and processes of the organization, in consultation with appropriate stakeholders.

The information provided in the treatment plan should include:

— the rationale for selection of the treatment options, including the expected benefits to be gained;

— those who are accountable and responsible for approving and implementing the plan;

— the proposed actions;

— the resources required, including contingencies;

— the performance measures;

— the constraints;

— the required reporting and monitoring;

— when actions are expected to be undertaken and completed.

## 6.6 Monitoring and review

The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes. Ongoing monitoring and periodic review of the risk management process and its outcomes should be a planned part of the risk management process, with responsibilities clearly defined.

Monitoring and review should take place in all stages of the process. Monitoring and review includes planning, gathering and analysing information, recording results and providing feedback.

The results of monitoring and review should be incorporated throughout the organization's performance management, measurement and reporting activities.

## 6.7 Recording and reporting

The risk management process and its outcomes should be documented and reported through appropriate mechanisms. Recording and reporting aims to:

— communicate risk management activities and outcomes across the organization;

— provide information for decision-making;

— improve risk management activities;

— assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.


© ISO 2018 – All rights reserved

Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

Decisions concerning the creation, retention and handling of documented information should take into account, but not be limited to: their use, information sensitivity and the external and internal context.

Reporting is an integral part of the organization's governance and should enhance the quality of dialogue with stakeholders and support top management and oversight bodies in meeting their responsibilities. Factors to consider for reporting include, but are not limited to:

— differing stakeholders and their specific information needs and requirements;

— cost, frequency and timeliness of reporting;

— method of reporting;

— relevance of information to organizational objectives and decision-making.

Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

© ISO 2018 – All rights reserved

# Bibliography

[1] IEC 31010, *Risk management — Risk assessment techniques*


© ISO 2018 – All rights reserved

Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by  University of Toronto User.  No further reproduction or distribution is permitted.

Copyrighted material licensed to University of Toronto by Clarivate Analytics (US) LLC, subscriptions.techstreet.com, downloaded on 2018-03-11 14:38:32 -0500 by University of Toronto User. No further reproduction or distribution is permitted.

**ICS 03.100.01**

Price based on 16 pages

© ISO 2018 – All rights reserved